THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

ARIANA SKURAUSKIS, RENEE ROGERS, and NOAH ROGERS, on behalf of themselves and all others similarly situated, Plaintiffs, v. **SANTA CLARA FAMILY HEALTH PLAN** **and** **NATIONSBENEFITS HOLDINGS, LLC,** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Ariana Skurauskis, Renee Rogers, and Noah Rogers, individually and on behalf of all similarly situated persons, allege the following against Santa Clara Family Health Plan ("SCFHP") and NationsBenefits Holdings, LLC ("NationsBenefits") (collectively, "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated SCFHP members'("Class Members")

personally identifiable information ("PII") and protected health information ("PHI"), including name, address, phone number, gender, date of birth, health insurance number, medical ID number, Social Security number, date(s) of service, medical device or product purchased, and provider/caregiver name (the "Private Information"),[1] from unauthorized disclosure to cybercriminals.

2. Defendant SCFHP is a community-based health plan located in San Jose, California serving more than 320,000 people through its various product offerings, including Medi-Cal, Cal MediConnect, and SCFHP DualConnect healthcare plans.

3. NationsBenefits provides supplemental benefits administration services to several health plans, including SCFHP.

4. Plaintiffs bring this class action lawsuit to address Defendants' collective inadequate safeguarding and supervision of Class Members' Private Information that they collected and maintained, and their failure to adequately supervise their business associates, vendors, and/or suppliers and timely detect the Data Breach.

5. On or about January 30, 2023 or earlier, an unauthorized third party or person accessed and downloaded Plaintiffs' and Class Members' Private Information. Both Defendants have independent, non-delegable duties to their members to safeguard their PHI and PII and are responsible for the wrongful disclosure of Plaintiffs' and Class Members' Private Information.

6. On February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra, LLC ("Fortra") disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers used "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

[1] *See* https://www.hipaajournal.com/277000-santa-clara-family-health-plan-members-affected-by-goanywhere-hack/ (last visited on April 30, 2023).

7. On or around February 10, 2023, the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT, and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days.

8. On February 22, 2023, the U.S. Department of Health and Human Services' ("HHS") Health Sector Cybersecurity Coordination Center issued a "Sector Alert" emphasizing that Clop's claim referenced its ability to target health care systems.

9. On March 30, 2023, Defendants confirmed that the PII and PHI of certain members, including Plaintiffs, were exposed by Fortra's attacker (the "Data Breach"). NationsBenefits estimates that approximately 3,037,303 members were impacted by the Data Breach.[2]

10. Upon information and belief, the vulnerability in Defendants' internal file transfer system was discovered by Defendants on or before January 29, 2023.[3] Thus, Defendants could have prevented the Data Breach, yet Defendants' business associate had to inform Defendants of the Data Breach (despite Defendants' knowledge of the vulnerability) after the compromise and exfiltration of Plaintiffs' and Class Members' Private Information had already occurred.

11. Defendants also could have prevented this theft had they limited the member information they shared with their business associates and employed reasonable supervisory measures to ensure that adequate data security practices, procedures, and protocols were being implemented and maintained by said business associates in order to secure and protect Defendants' members' data.

12. Defendants failed to comply with industry standards to protect members' Private Information and failed to provide adequate notice to Plaintiffs and other Class Members that their

[2] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited on May 3, 2023).

[3] *See* https://www.techtarget.com/searchsecurity/news/365535543/Fortra-completes-GoAnywhere-MFT-investigation (last visited on May 3, 2023).

PII and PHI had been compromised. Plaintiffs seek, among other things, orders requiring Defendants to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breach in the future.

13. Plaintiffs and Class Members would not have provided their Private Information to Defendants if they had known that Defendants would breach their promises and agreements by (a) failing to ensure that their vendors used adequate security measures, and/or (b) providing members' PII and PHI to business associates that utilized inadequate security measures.

14. Armed with the Private Information accessed in the Data Breach, data thieves can and will commit a variety of crimes against Plaintiffs and Class Members, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

16. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, including out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

17. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding and supervision of Class Members' Private Information that they collected and maintained. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, thus Defendants were on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

18. Upon information and belief, Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. Had they properly monitored their networks and provided adequate supervision over their agents, vendors, and/or suppliers, they would have discovered the system vulnerability at issue sooner and prevented the Data Breach.

19. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that Defendants collected and maintained is now in the hands of data thieves and other unauthorized third parties.

20. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

II. PARTIES

21. Plaintiff Ariana Skurauskis is, and at all times mentioned herein was, an individual citizen of the State of California.

22. Plaintiff Renee Rogers is, and at all times mentioned herein was, an individual citizen of the State of California.

23. Plaintiff Noah Rogers is, and at all times mentioned herein was, an individual citizen of the State of California.

24. Defendant SCFHP is a community-based health plan located at 6201 Ignacio Ave., San Jose, California 95119.

25. Defendant NationsBenefits is, upon information and belief, a nationwide company with offices throughout the country, with its principal place of business located at 1801 NW 66th Ave., Suite 100, Plantation, FL 33312.

III. JURISDICTION AND VENUE

26. This Court has jurisdiction over the parties and the subject matter of this action. Jurisdiction is proper because Defendant NationsBenefits is a corporation operating throughout the nation whose principal place of business is in the state of Florida and because SCFHP conducts business in and has sufficient minimum contacts with the State of Florida, including but not limited to, through its sharing of members' personal information with NationsBenefits and working with NationsBenefits to attempt to keep such information private and secure.

27. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendant.

28. Venue is proper in this District because the acts and omissions complained of herein occurred (and Defendant NationsBenefits is located) within this District. Upon information and belief, Plaintiffs' and Class Members' Private Information was also being maintained within this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Business and Collection of Plaintiffs' and Class Members' Private Information

29. Founded in 1997, SCFHP is a community-based health plan located in San Jose, California serving more than 320,000 people through its various product offerings, including Medi-Cal, Cal MediConnect, and DualConnect healthcare plans.

30. SCFHP employs more than 241 people and generates approximately $75 million in annual revenue.

31. NationsBenefits, with its headquarters in Plantation, Florida, serves "millions of members" as a "leading provider of supplemental benefits, flex cards, and member engagement solutions that partners with managed care organizations to provide innovative healthcare solutions designed to drive growth, improve outcomes, reduce costs, and delight members."[4]

32. NationsBenefits employs over 3,500 employees in locations that span across the United States.[5]

33. As a condition of receiving healthcare plans and services, Defendants require that members turn over highly sensitive personal and health information. In the ordinary course of receiving service from Defendants, Plaintiff and Class Members were required to provide their Private Information to them.

34. In its Notice of Privacy Practices (also referred to herein as the "Privacy Policy"), SCFHP makes clear that it is "required by state and federal law to protect your health information."[6] SCFHP also describes in its Privacy Policy the limited specific instances when it

[4] *See* https://www.nationsbenefits.com/about-us (last visited on April 30, 2023).

[5] *Id.*

[6] *See* https://www.scfhp.com/privacy-policy/#:~:text=Your%20Information%20is%20Personal%20and,pay%20for%20your%20health%20care. (last visited on April 28, 2023).

shares patient health information and says that in order for such sharing to occur, "we must get your written permission."[7]

35. SCFHP uses this information, *inter alia*, "[f]or treatment," "[f]or payment," "[f]or health care operations," and "[f]or business associates … that assist[] us in operating our health system."[8]

36. In NationsBenefits' Privacy Policy, it promises to only share or Plaintiffs' and Class Members' Private Information "when you have given consent; where the sharing or disclosure is necessary or required by law; where the sharing of information is provided to trusted entities who work on behalf of or with NationsBenefits under strict confidentiality agreements in order to help NationsBenefits communicate with you; when sharing the information is believed to be reasonably necessary to investigate, prevent, or take action against any suspected or actual illegal activities and threats; if NationsBenefits is acquired by, merged with, or acquires another company; with our affiliates for internal business purposes."

37. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties owed to them and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

38. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

[7] *Id.*

[8] *Id.*

B. The Data Breach

39. Fortra was one of Defendants' "business associates." Nevertheless, on February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. Hackers used "remote code injection exploits" to remotely execute malicious code on their targets' computer systems.

40. On or around February 10, 2023, the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT, and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days.

41. On March 30, 2023, SCFHP reported that it was one of the entities impacted, and that the PII and PHI of certain of its members were exposed by Fortra's attacker. NationsBenefits filed an official report with the United States Department of Human Health and Services Office for Civil Rights confirming that over 3 million of their members', including Plaintiffs', Private Information was compromised as a result of the Data Breach.

42. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including medical records, Social Security numbers, past and current medications and health insurance information.

43. Defendants delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed.

44. Defendants had obligations created by contract, industry standards, common law, federal and state regulations, and representations made to Plaintiff and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such Information confidential and secure from unauthorized access.

46. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

47. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

48. Defendants were on notice that companies in the healthcare industry are susceptible targets for data breaches.

49. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[9]

50. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting confidential medical information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of

[9] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on April 28, 2023).

> patients' health and financial information, but also patient access to care.[10]

51. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[11] In 2022, the largest growth in compromises occurred in the healthcare sector.[12]

52. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13]

53. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[14]

---

[10] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on April 28, 2023).

[11] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on April 28, 2023).

[12] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on April 28, 2023).

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on April 28, 2023).

[14] *Id.*

54. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[15]

55. Defendants knew, or should have known, the importance of safeguarding their members' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on their members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Defendants Failed to Comply with HIPAA

56. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

57. The Data Breach resulted from a combination of insufficiencies that indicate Defendants failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from the Data Breach that Defendants either failed to implement,

[15] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on April 28, 2023).

or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

58. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

59. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

60. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

61. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

62. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

63. Based upon SCFHP's Notice to Plaintiff and Class Members, Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

64. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

65. Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR,

Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

66. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

67. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

68. Defendants reasonably believe that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

69. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

70. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

71. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

72. Defendants' security failures also include, but are not limited to:

a. Failing to maintain adequate data security systems, practices, and protocols to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity *or business associate* creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added).

d. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy

rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3); and

i. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

73. Because Defendants have failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendants' approach to information security, especially as such approach relates to the supervision of their business associates, vendors, and/or suppliers, is adequate and appropriate going forward. Defendants still maintain the PHI and other highly sensitive PII of their current and former members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Defendants Failed to Comply with FTC Guidelines

74. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

75. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep,

properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

76. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

77. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

78. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

79. Defendants were at all times fully aware of their obligation to protect the Private Information of their members yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' Private Information

80. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols (and those of their business associates, vendors, and/or suppliers) adequately protected the Private Information of Class Members.

81. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data (and those of their business associates, vendors, and/or suppliers). Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect members' Private Information;

b. Failing to sufficiently train and monitor their business associates, vendors, and/or suppliers regarding the proper handling of their members' Private Information;

c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

d. Failing to adhere to HIPAA and industry standards for cybersecurity, as discussed above; and

e. Otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' Private Information.

82. Had Defendants remedied the deficiencies in their information storage and security practices, procedures, and protocols, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented the theft of Plaintiffs' and Class Members' confidential Private Information.

83. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

G. Defendants Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

84. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[16] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

85. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[16] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on April 28, 2023).

86. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

87. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

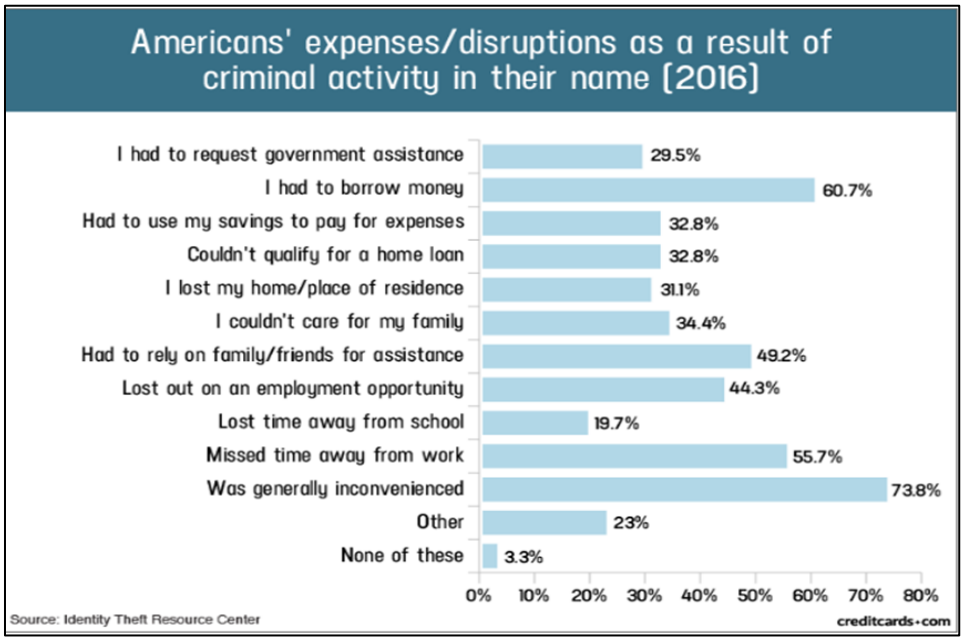
88. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

89. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

freeze on their credit, and correcting their credit reports.[17] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

90. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

91. In fact, a study by the Identity Theft Resource Center[18] shows the multitude of harms caused by fraudulent use of PII:



[17] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited April 28, 2023).

[18] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on April 28, 2023).

92. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[19]

93. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

94. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[20]

95. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

96. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial

[19] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on April 28, 2023).

[20] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on April 28, 2023).

repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

97. The ramifications of Defendants' failure to keep their members' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

98. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

99. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[22]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[21] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on April 28, 2023).

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 28, 2023).

100. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

101. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Damages

102. Plaintiff Skurauskis began utilizing Defendants' services in or around the year of 2014 and, as a result, was required to disclose her Private Information to Defendants.

103. Plaintiff Renee Rogers began utilizing Defendants' service in or around the year of 2012 and, as a result, was required to disclose her Private Information to Defendants.

104. Plaintiff Noah Rogers began utilizing Defendants' service in or around the year of 2012 and, as a result, was required to disclose his Private Information to Defendants.

105. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

106. Plaintiffs and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

107. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices, procedures, and protocols, as discussed herein.

108. As a direct and proximate result of Defendants' actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names,

loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

109. These harms are not just hypothetical. Plaintiff Skurauskis has already been the victim of the fraudulent misuse of her information, as cybercriminals have utilized her stolen Private Information to access her online accounts and attempt to make unauthorized purchases in her name.

110. Further, as a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been forced to expend time dealing with and attempting to mitigate the negative effects thereof.

111. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

112. The Private Information maintained by and stolen from Defendants' system, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against them, as has already been the case with Plaintiff Skurauskis.

113. Additionally, Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and records, including medical records and explanations of benefits, for misuse.

114. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the

value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

j. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

115. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants and their business associates, vendors, and/or suppliers, is protected from future breaches by the implementation of more adequate data security measures and safeguards.

116. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

117. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23.

118. Specifically, Plaintiffs propose the following Nationwide Class and California Subclass (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All persons residing in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **California Subclass**
>
> All California citizens who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

119. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

120. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

121. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact identities of Class Members are unknown at this time, based on information and belief, the Class consists of roughly 3,037,303 individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through

Defendants' records, Class Members' records, publication notice, self-identification, and other means.

122. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA, HIPAA, and/or the CMIA, the CLRA, or California's unfair competition law;

c. Whether and to what extent Defendants had a duty to protect the Private Information of Class Members;

d. When Defendants learned of the vulnerability within NationsBenefits' network that led to the Data Breach;

e. Whether Defendants' response to the Data Breach was adequate;

f. Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' Private Information;

g. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

h. Whether hackers obtained Class Members' Private Information via the Data Breach;

i. Whether Defendants knew or should have known that their data monitoring and supervision processes were deficient;

j. Whether Defendants were aware that their business associates', vendors', and/or suppliers' data security practices, procedures, and protocols were inadequate;

k. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;

l. Whether Defendants' conduct was negligent;

m. Whether Defendants were unjustly enriched;

n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

o. Whether Plaintiffs and Class Members are entitled to lifetime credit or identity monitoring and monetary relief; and

p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

123. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

124. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

125. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way and as a result of the same negligent acts and omissions committed by Defendants. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

126. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

127. Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

128. Finally, all members of the proposed Class are readily ascertainable. Defendants has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE CALIFORNIA SUBCLASS)

129. Plaintiffs restate and reallege all of the allegations in paragraphs 1-128 as if fully set forth herein.

130. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

131. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, they knew or should have known that the Private Information would be an attractive target for cyberattacks.

132. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, supervising, monitoring, and protecting the Private Information in their possession;

b. To protect members' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA, the California Confidentiality of Medical Information Act ("CMIA"), California Customer Records Act ("CCRA"), and California Unfair Competition Law ("UCL");

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

133. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

134. Defendants' duty also arose because Defendants were bound by industry standards to protect their members' confidential Private Information.

135. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants and their associates, vendors, and/or suppliers, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

136. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within their care.

137. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate data security practices to safeguard the Private Information of Plaintiffs and Class Members.

138. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of the Private Information;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA;

e. Failing to comply with HIPAA; and

f. Failing to comply with other state laws and regulations, as further set forth herein.

139. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions.

140. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

141. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

142. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

143. As a result of Defendants' negligence in breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

144. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

145. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

146. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

147. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

148. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security monitoring procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE CALIFORNIA SUBCLASS)

149. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

150. Plaintiffs and Class Members entered into a valid and enforceable contract through which they were required to turn over their Private Information to Defendants in exchange for services. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information to any third parties without their consent.

151. Defendants' Privacy Policy memorialized the rights and obligations of Defendants and their members. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

152. In their Privacy Policy(ies), Defendants commit to protecting the privacy and security of the Private Information and promise to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

153. Plaintiffs and Class Members fully performed their obligations under their contracts with Defendants.

154. However, Defendants did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore Defendants breached their contracts with Plaintiffs and Class Members.

155. Defendants allowed criminal third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, Defendants breached their contracts with Plaintiffs and Class Members.

156. Defendants' failure to satisfy their confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and state laws and regulations, resulted in Defendants providing services to Plaintiffs and Class Members that were of a diminished value and in breach of their contractual obligations to Plaintiffs and Class Members.

157. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendants' failure to fully perform their part of the agreement with Plaintiffs and Class Members.

158. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

159. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security monitoring procedures, conduct periodic audits of those procedures, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE CALIFORNIA SUBCLASS)

160. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

161. This Count is pleaded in the alternative to Count II above.

162. Defendants provide healthcare plans and services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendants regarding the provision

of those services through their collective conduct, including by Plaintiffs and Class Members providing their Private Information to Defendants in exchange for the services offered.

163. Through Defendants' offering of healthcare plans and services, they knew or should have known that they needed to protect Plaintiffs' and Class Members' confidential Private Information in accordance with Defendants' policies, practices, and applicable state and federal law.

164. As consideration, Plaintiffs and Class Members turned over valuable Private Information to Defendants. Accordingly, Plaintiffs and Class Members bargained with Defendants to securely maintain and store their Private Information.

165. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

166. In delivering their Private Information to Defendants in exchange for Defendants' services, Plaintiffs and Class Members intended and understood that Defendants would adequately safeguard the Private Information as part of those services.

167. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information, including their business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of their business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA

standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

168. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

169. Had Defendants disclosed to Plaintiffs and the Class that they did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

170. As a provider of healthcare plans and services, Defendants recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the Class.

171. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Defendants further breached these implied contracts by failing to comply with their promise to abide by HIPAA.

172. Additionally, Defendants breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information they created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

173. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

174. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

175. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

176. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

177. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce violations, in violation of 45 CFR 164.306(a)(94).

178. Defendants further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

179. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

180. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality, integrity, and availability of all electronic

protected health information their business associate(s) create, receive, maintain, or transmit" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added)

181. Defendants further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

182. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendants in exchange for Defendants' agreement to, *inter alia*, protect their Private Information.

183. Plaintiffs and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *ET SEQ.*
(ON BEHALF OF PLAINTIFFS AND THE CALIFORNIA SUBCLASS)

184. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

185. Defendants are "provider[s] of healthcare" services as defined in Cal. Civ. Code § 56.06, and are therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

186. Plaintiffs and the Class are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

187. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code

§ 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the inactions of Defendants, including their failure to adequately implement sufficient data security and monitoring measures and protocols to protect Plaintiffs' and Class Members' Private Information, which allowed hackers to obtain such Information.

188. Specifically, Defendants' negligence resulted in the release of individually identifiable PHI pertaining to Plaintiffs and the Class to unauthorized cybercriminals and the breach of the confidentiality of that information. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class Members' Private Information in a manner that preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

189. Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information belonging to Plaintiffs and the Class, in violation of Cal. Civ. Code § 56.101(b)(1)(A).

190. Plaintiffs and the Class were injured and have suffered damages, as described above, from Defendants' illegal disclosure and negligent acts and omissions resulting in the release of their medical information, in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT V
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. PROF. CODE § 17200, *ET SEQ.*
(ON BEHALF OF PLAINTIFFS AND THE CALIFORNIA SUBCLASS)

191. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

192. Defendants violated California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. By representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class Members' Private Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that Defendants would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiffs' and the Class's Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. By soliciting and collecting Private Information from Plaintiffs' and Class Members without adequately protecting or storing Private Information;

c. By violating the privacy and security of HIPPA, 42 U.S.C. §1302d, *et seq*.; and

d. By violating the CMIA, Cal. Civ. Code § 56, *et seq*.

193. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq*., and the CMIA, Cal. Civ. Code § 56, *et seq*.

194. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, Plaintiffs and the Class were injured and lost money and property, including but not limited

to, the loss of their legally protected interest in the confidentiality and privacy of their Private Information, including PHI, and additional losses described above.

195. Defendants knew or should have known that their data security practices, procedures, and protocols were inadequate to safeguard Plaintiffs' and Class Members' Private Information and that the risk of theft was highly likely. Defendants had resources to secure and/or prepare for protecting patient Private Information in a Data Breach. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

196. Plaintiffs seek relief under the UCL, including restitution to the Class of money or property that the Defendants may have acquired by means of Defendants' deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

COUNT VI
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

197. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

198. This Count is pleaded in the alternative to Counts II and III above.

199. Plaintiffs and Class Members conferred a benefit on Defendants. Specifically, they provided Defendants with their Private Information, which Private Information has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to Defendants' adequate protection and supervision of their Private Information, especially in light of their special relationship.

200. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

201. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

202. Defendants acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

203. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative choices that excluded Defendants.

204. Plaintiffs and Class Members have no adequate remedy at law.

205. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

206. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching

how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

207. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

208. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VII
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE CALIFORNIA SUBCLASS)

209. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

210. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendants and ultimately accessed and acquired in the Data Breach.

211. As a healthcare plan and services provider, Defendants have a special relationship with their members, including Plaintiffs and Class Members. Because of that special relationship, Defendants was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to ensure that such was maintained in confidence.

212. Members like Plaintiffs and Class Members have a privacy interest in personal medical and other matters, and Defendants had a duty not to permit the disclosure of such matters concerning their members.

213. As a result of the parties' relationship, Defendants had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

214. Plaintiffs and Class Members did not consent nor authorize Defendants to release or disclose their Private Information to an unknown criminal actor.

215. Defendants breached their duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) mismanaging their system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (d) failing to follow their own privacy policies and practices published to their members; and (e) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

216. But for Defendants wrongful breach of their duty of confidence owed to Plaintiff and Class Members, their Private Information would not have been compromised.

217. As a direct and proximate result of Defendants' wrongful breach of their duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

218. It would be inequitable for Defendants to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

219. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VIII
INJUNCTIVE/DECLARATORY RELIEF
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE CALIFORNIA SUBCLASS)

220. Plaintiffs restate and reallege the allegations in paragraphs 1-128 as if fully set forth herein.

221. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

222. Defendants owe a duty of care to Plaintiffs and Class Members, which required them to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

223. Defendants and their associates, vendors, and/or suppliers still possess the Private Information belonging to Plaintiffs and Class Members.

224. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

225. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure their members' Private Information under the common law, HIPAA, the FTCA, and the CMIA;

b. Defendants' existing data monitoring measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect members' Private Information; and

c. Defendants continues to breach this legal duty by failing to employ reasonable measures to secure members' Private Information.

226. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their users about the threats they face with regard to the security of their Private Information, as well as the steps Defendants' members should take to protect themselves.

227. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs will

not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

228. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

229. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendants, thus preventing future injury to Plaintiffs and other members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the California Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: May 4, 2023

Respectfully submitted,

/s/ Jessica Wallace
Jessica Wallace, Bar No. 1008325
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: jwallace@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com